EXPERIMENT-2

NAME:KALAIYARASI.M **ROLL NO: 231901048**

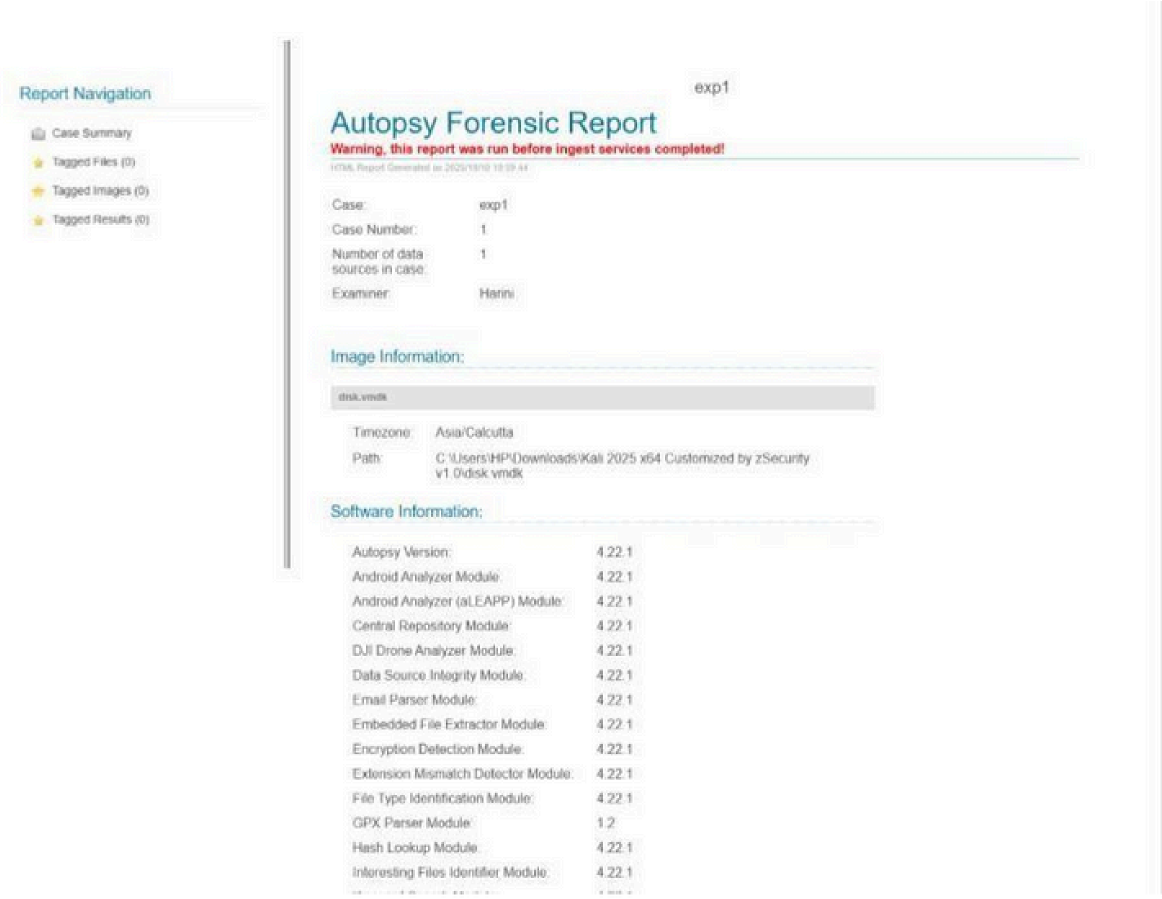
Aim :

Live Forensics Case Investigation using Autopsy .

Here is the procedure and expected result for Experiment 2 (Live Forensics Case Investigation usingAutopsy):

Procedure :

1. **Download andInstallAutopsy:**
   - o ObtainAutopsyfromtheofficial website and install it on your PC.
2. **Create a NewCase:**
   - o LaunchAutopsy,select“NewCase”.
   - o Enteracasename,basedirectory, and specify report location.
3. **Enter Case Details:** o Fillincase number and examiner details, then click Finish.
4. **Add Data Source:**
   - o In thenewwindow,choose“Add Data Source”.
   - o Browsetothefilepathofyourevidence (disk image, device, etc.) and add it.
5. **Configure IngestModules:**
   - o Selectallingestmodulestoperform a comprehensive investigation (file analysis,extractingartifacts,operating system info, user accounts, web history, downloads,cookies,emailaddresses, and more).
6. **Start Investigation:**
   - o ClickFinishinAddDataSource. Autopsy will process the data and add it to the localdatabase.
7. **Explore InvestigationResults:**
   - o After processing,reviewoutputs by clicking on:
     - **DevicesAttached**:Seeconnected devices.
     - **EXIFMetadata**:Inspect image info.
     - **InstalledPrograms**:View programs on the system.
     - **Operating System Information**: Analyze OS details.
     - **Operating System User Account**: List user accounts.
     - **Recent Documents**: Find recently opened docs.
     - **Web Bookmarks/History/Downloads/Search/Cookies**: Analyze user browsing artifacts.
     - **Email addresses**: Review found emails.



exp1

Autopsy Forensic Report

Warning, this report was run before ingest services completed!

HTML Report Generated at 2025/10/10 10:59:44

Case:	exp1
Case Number:	1
Number of data sources in case:	1
Examiner:	Harini

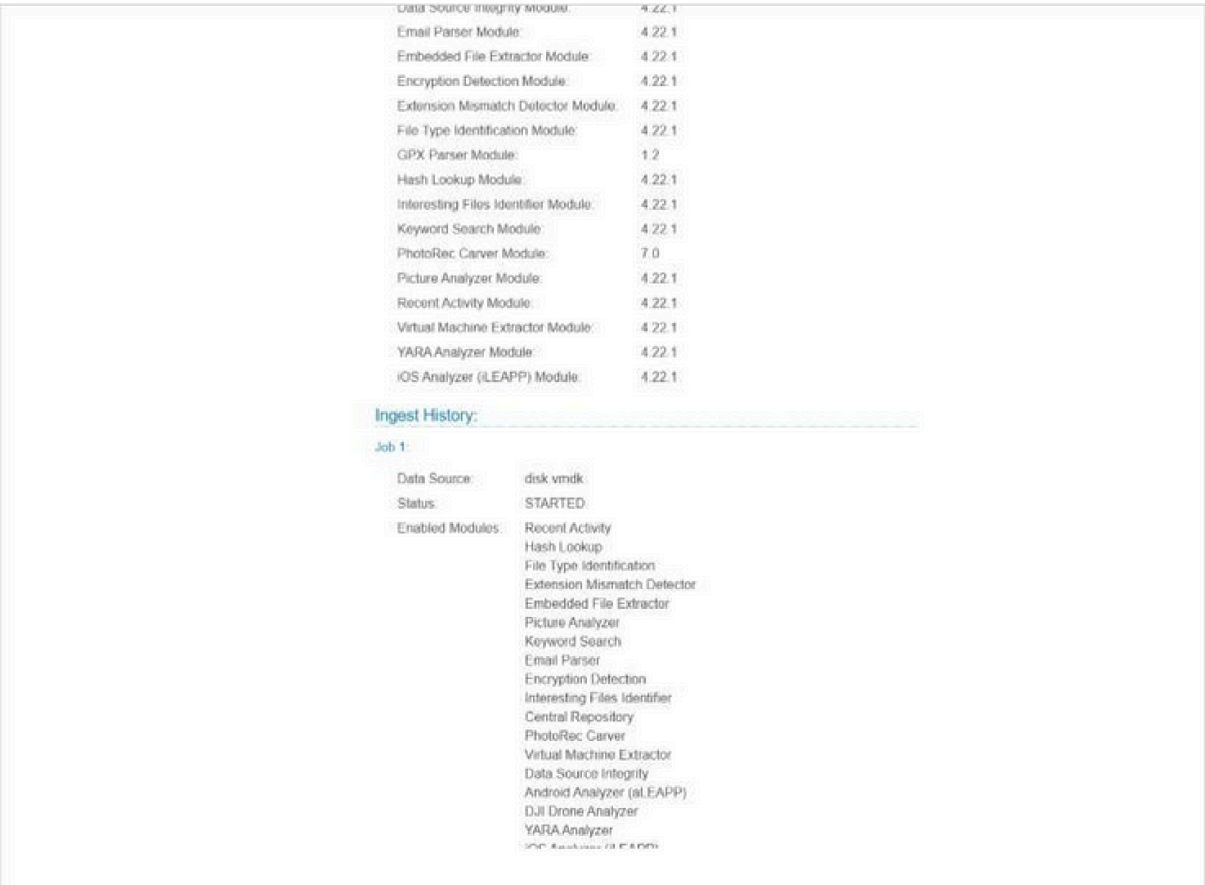
Image Information:

disk.vmdk

Timezone:	Asia/Calcutta
Path:	C:\Users\HP\Downloads\Kali 2025 x64 Customized by zSecurity v1.0\disk.vmdk

Software Information:

Autopsy Version:	4.22.1
Android Analyzer Module:	4.22.1
Android Analyzer (aLEAPP) Module:	4.22.1
Central Repository Module:	4.22.1
DJI Drone Analyzer Module:	4.22.1
Data Source Integrity Module:	4.22.1
Email Parser Module:	4.22.1
Embedded File Extractor Module:	4.22.1
Encryption Detection Module:	4.22.1
Extension Mismatch Detector Module:	4.22.1
File Type Identification Module:	4.22.1
GPX Parser Module:	1.2
Hash Lookup Module:	4.22.1
Interesting Files Identifier Module:	4.22.1



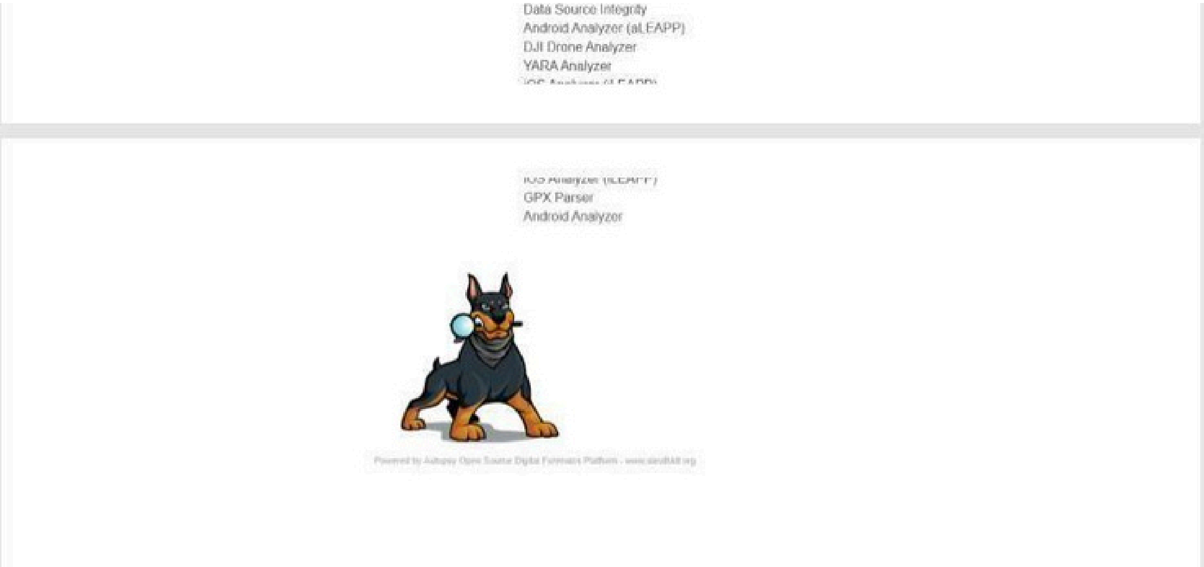
Data Source Integrity Module:	4.22.1
Email Parser Module:	4.22.1
Embedded File Extractor Module:	4.22.1
Encryption Detection Module:	4.22.1
Extension Mismatch Detector Module:	4.22.1
File Type Identification Module:	4.22.1
GPX Parser Module:	1.2
Hash Lookup Module:	4.22.1
Interesting Files Identifier Module:	4.22.1

Keyword Search Module:	4.22.1
PhotoRec Carver Module:	7.0
Picture Analyzer Module:	4.22.1
Recent Activity Module:	4.22.1
Virtual Machine Extractor Module:	4.22.1
YARA Analyzer Module:	4.22.1
iOS Analyzer (iLEAPP) Module:	4.22.1

Ingest History:

Job 1:

Data Source:	disk.vmdk
Status:	STARTED
Enabled Modules:	Recent Activity Hash Lookup File Type Identification Extension Mismatch Detector Embedded File Extractor Picture Analyzer Keyword Search Email Parser Encryption Detection Interesting Files Identifier Central Repository PhotoRec Carver Virtual Machine Extractor Data Source Integrity Android Analyzer (aLEAPP) DJI Drone Analyzer YARA Analyzer iOS Analyzer (iLEAPP)



Data Source Integrity
Android Analyzer (aLEAPP)
DJI Drone Analyzer
YARA Analyzer
iOS Analyzer (iLEAPP)
GPX Parser
Android Analyzer

Powered by Autopsy Open Source Digital Forensics Platform - www.sleuthkit.org

Result:

Thus, theforensic tools executed successfully, and the evidence was captured and analyzed accurately.